

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-181689

(43)Date of publication of application : 12.07.1996

(51)Int.Cl.

H04L 9/00
H04L 9/10
H04L 9/12
H04H 1/00
H04N 7/167

(21)Application number : 07-030056

(71)Applicant : SONY CORP

(22)Date of filing : 25.01.1995

(72)Inventor : KUBOTA YUKIO
GOTO KOICHI

(30)Priority

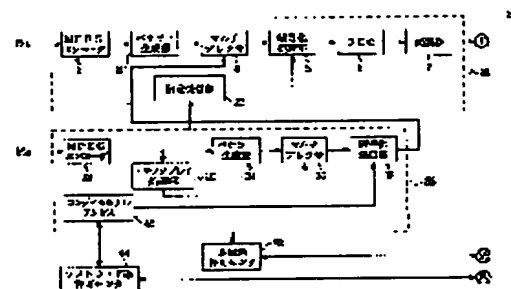
Priority number : 06289139 Priority date : 28.10.1994 Priority country : JP

(54) DIGITAL SIGNAL TRANSMISSION METHOD, DIGITAL SIGNAL RECEIVER AND RECORDING MEDIUM

(57)Abstract:

PURPOSE: To remarkably improve the security by applying 1st ciphering to a digital signal obtained by applying band compression coding to a video signal, applying ciphering further to the processed signal and sending the resulting signal.

CONSTITUTION: A software supply section 32 uses an MPEG encoder 33 to apply band compression coding to software data PS2 of a digital signal. A trick play section 35 applies processing to extract a picture from video data and provides an output to a multiplexer 36. The digital signal multiplexed by the multiplexer 36 is subject to ciphering of a storage group by a ciphering section 37 and the result is sent to a multiplexer 4 of a transmission section 31. The multiplexer 4 multiplexes the digital signal and a ciphering section 5 applies ciphering of a broadcast group to the multiplexed signal. The digital signal with duplicate security is sent to a digital signal receiver from a satellite.



LEGAL STATUS

[Date of request for examination] 30.03.2000

[Date of sending the examiner's decision of rejection] 25.10.2002

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3729529

[Date of registration] 14.10.2005

[Number of appeal against examiner's decision of rejection] 2002-22757

[Date of requesting appeal against examiner's] 25.11.2002

Searching PAJ

페이지 2 / 2

decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-181689

(43) 公開日 平成8年(1996)7月12日

(51) Int.Cl.⁶H 0 4 L 9/00
9/10
9/12

識別記号

庁内整理番号

F I

技術表示箇所

H 0 4 L 9/ 00

Z

H 0 4 N 7/ 167

審査請求 未請求 請求項の数 9 F D (全 15 頁) 最終頁に続く

(21) 出願番号 特願平7-30056

(22) 出願日 平成7年(1995)1月25日

(31) 優先権主張番号 特願平6-289139

(32) 優先日 平6(1994)10月28日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 久保田 幸雄

東京都品川区北品川6丁目7番35号ソニー
株式会社内

(72) 発明者 後藤 晃一

東京都品川区北品川6丁目7番35号ソニー
株式会社内

(74) 代理人 弁理士 田辺 恵基

(54) 【発明の名称】 デジタル信号伝送方法、デジタル信号受信装置及び記録媒体

(57) 【要約】

【目的】 本発明は、デジタル信号伝送方法、デジタル信号受信装置及び記録媒体について、有料のソフトウェア情報のセキュリティを確保する。

【構成】 所定のサービスを提供する映像を伝送する場合、映像信号を帯域圧縮符号化したデジタル信号に第1の暗号化処理をした後、当該デジタル信号にさらに暗号化処理をして伝送する。これにより映像信号に2重のセキュリティを付加することかできるので、一段とセキュリティが確保されたデジタル信号伝送方法を実現し得る。

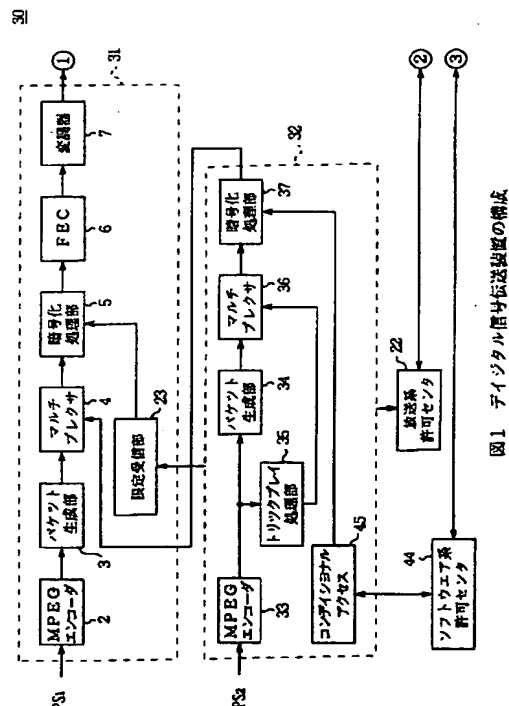


図1 デジタル信号伝送装置の構成

【特許請求の範囲】

【請求項 1】少なくとも映像信号を帯域圧縮符号化したデジタル信号に暗号化処理をして伝送するデジタル信号伝送方法において、

所定のサービスを提供する映像を伝送する場合には、上記帯域圧縮符号化したデジタル信号に第 1 の暗号化処理をした後、当該第 1 の暗号化処理がなされたデジタル信号にさらに上記暗号化処理をして伝送することを特徴とするデジタル信号伝送方法。

【請求項 2】上記帯域圧縮符号化されかつ第 1 の暗号化処理がなされたデジタル信号と、所定映像単位内で上記帯域圧縮符号化が完結しているデジタル信号とを混合し、

当該混合信号に上記暗号化処理をして伝送することを特徴とする請求項 1 に記載のデジタル信号伝送方法。

【請求項 3】上記帯域圧縮符号化したデジタル信号に上記第 1 の暗号化処理をする際に用いる第 1 の暗号化キーを第 2 の暗号化キーを用いて暗号化することを特徴とする請求項 1 に記載のデジタル信号伝送方法。

【請求項 4】少なくとも映像信号を帯域圧縮符号化したデジタル信号に暗号化処理をして伝送するデジタル信号伝送方法において、

上記帯域圧縮符号化されかつ暗号化処理がなされたデジタル信号と、所定映像単位内で上記帯域圧縮符号化が完結しているデジタル信号とを混合して伝送することを特徴とするデジタル信号伝送方法。

【請求項 5】少なくとも映像信号を帯域圧縮符号化したデジタル信号に第 1 の暗号をかけた後、第 2 の暗号をかけて放送局より伝送されるデジタル信号を受信するデジタル信号受信装置において、

上記デジタル信号にかけられた上記第 2 の暗号を解除する第 2 の暗号解除手段と、

当該第 2 の暗号が解除されたデジタル信号を記録媒体に記録すると共に、当該記録媒体に記録されたデジタル信号を再生する記録再生手段と、

上記記録媒体より再生される再生信号の上記第 1 の暗号を解除する第 1 の暗号解除手段とを具えることを特徴とするデジタル信号受信装置。

【請求項 6】上記第 1 の暗号解除手段は、上記帯域圧縮符号化したデジタル信号に上記第 1 の暗号をかける際に用いる暗号化キーにかけられている暗号を解除する暗号化キー用の暗号解除手段を具え、当該暗号化キー用の暗号解除手段によつて上記暗号化キーにかけられている暗号を解除し、当該暗号が解除された暗号化キーを用いて上記再生信号の第 1 の暗号を解除することを特徴とする請求項 5 に記載のデジタル信号受信装置。

【請求項 7】上記放送局は、帯域圧縮符号化したデジタル信号に第 1 の暗号をかけたデジタル信号と所定映像単位内で上記帯域圧縮符号化が完結しているデジタル信号とを混合して当該混合信号に第 2 の暗号をかけて

伝送し、

上記記録再生手段は、上記第 1 の暗号がかけられたデジタル信号と所定映像単位内で上記帯域圧縮符号化が完結しているデジタル信号とを記録し、変速再生時には、上記所定映像単位内で上記帯域圧縮符号化が完結しているデジタル信号を用いて変速再生画を出力することを特徴とする請求項 5 に記載のデジタル信号受信装置。

【請求項 8】モデムを有し、課金情報を管理する複数の管理局へのアクセスの切換えを上記モデムを介して制御することにより、上記複数の課金体系を構築することを特徴とするデジタル信号受信装置。

【請求項 9】少なくとも映像信号を帯域圧縮符号化したデジタル信号に暗号化処理をしたデジタル信号が記録されていることを特徴とする記録媒体。

【発明の詳細な説明】

【 0 0 0 1 】

【目次】以下の順序で本発明を説明する。

産業上の利用分野

従来の技術（図 9 ～ 図 1 1）

発明が解決しようとする課題（図 1 1）

課題を解決するための手段（図 1、図 2 及び図 5 ～ 図 8）

作用（図 1、図 2 及び図 5 ～ 図 8）

実施例

（1）デジタル信号伝送装置及びデジタル信号受信装置の構成（図 1 及び図 2）

（2）実施例によるデジタル信号伝送装置の構成（図 3 及び図 4）

（3）実施例によるデジタル信号受信装置の構成（図 5 及び図 6）

（4）実施例によるデジタル信号伝送システム（図 7）

（5）他の実施例（図 8）

発明の効果

【 0 0 0 2 】

【産業上の利用分野】本発明はデジタル信号伝送方法、デジタル信号受信装置及び記録媒体に関し、例えば有料のソフトウェア情報を契約ユーザに提供するデジタル信号伝送システムに適用して好適なものである。

【 0 0 0 3 】

【従来の技術】従来、衛星又はケーブルによるデジタル信号伝送システムにおいては、図 9 に示すように、デジタル信号伝送装置すなわち放送局 1 において、入力されるプログラムソース P S を M P E G（Moving Picture Image Coding Experts Group）エンコーダ 2 で M P E G 方式で帯域圧縮符号化してパケット生成部 3 でパケット化する。

【 0 0 0 4 】パケット化された伝送データはマルチプレクサ 4 で多重化された後、暗号化処理部 5 で伝送データ

にセキュリティとしてスクランブルをかけ、さらにこのスクランブルが簡単に解けないように何重にも鍵（暗号）をかける。暗号化された伝送データは F E C (forward error correction) 部 6 でエラー訂正されて変調器 7 で変調された後、デジタル衛星 8 を介して契約ユーザの家庭内に設置されているデジタル信号受信装置すなわち端末 1 0 (図 1 0) に直接送出されるか、又は衛星 8 を介してヘッドエンドと呼ばれる配信局 9 (図 1 0) に送出され、配信局 9 よりケーブルを介して端末 1 0 に送出される。

【0005】ここで図 1 0 に示すように、端末 1 0 では、伝送データが衛星 8 を介して直接送られてきた場合には伝送データはアンテナ 1 1 で受信されてフロントエンド部 1 2 に送出され、伝送データが配信局 9 よりケーブルを介して送られてきた場合にはフロントエンドブロック 1 2 に直接入力される。放送局 1 と契約したユーザは、衛星 8 より直接又は衛星 8 より配信局 9 を介して送られてきた伝送データに対し、ユーザ毎に許可されたキーを端末 1 0 にアクセスすることにより、契約ユーザとしてオーソライズ（許可）されて課金処理されると同時に所望のソフトウェア情報を鑑賞することができる。

【0006】すなわち端末 1 0 において、チューナ、復調器及びエラー訂正器で構成されるフロントエンド部 1 2 で処理された伝送データはデータ取出し部 1 3 に入力される。データ取出し部 1 3 では、まずデマルチプレクサ 1 4 で多重化を解除して、映像信号、音声信号及びこれ以外のデータに分離する。暗号解除部 1 5 では、課金処理と同時に暗号を解除し、パケット分離部 1 6 でパケット分離した後、MPEG デコーダ 1 7 で圧縮を解凍（伸長）すると共にデジタル／アナログ変換して映像信号及び音声信号をテレビジョン（TV）に出力する。

【0007】

【発明が解決しようとする課題】ところでデジタル信号伝送システムでは、ビデオオンデマンド(video on demand) やニアビデオオンデマンド(near video on demand)などの有料のソフトウェア情報を伝送する場合、ユーザの便宜を図ると共にデジタル伝送路を有効に活用する手段として、端末 1 0 にテープメディアやディスクメディアのデジタルストレージ 1 8 を内蔵又は接続している。この場合、空き時間帯又は空き伝送路を利用して大容量のソフトウェアデータをストレージ 1 8 にダウンロードしておき、ユーザが手元のソフトウェア情報を観るときには、I D カード（例えばスマートカード） 1 9 でアクセスすることによって課金処理が行われて再生制限が解かれる。

【0008】すなわちユーザがスマートカード 1 9 でアクセスすると、中央処理装置（CPU） 2 0 がモデム 2 1 を介して許可センタ 2 2 (図 9) に登録の問い合わせを行う。許可センタ 2 2 は、コンディショナルアクセス (Conditional Access) 2 3 によって登録を確認し、登

録が確認されると、許可センタ 2 2 は課金処理をすると共にモデム 2 1 を介して CPU 2 0 に確認の通知を行う。

【0009】CPU 2 0 はこの通知によってローカルコンディショナルアクセス (Local Conditional Access) 2 4 にキーの解除を指示し、ローカルコンディショナルアクセス 2 4 はストレージ 1 8 に記録されているデータにかけられている暗号を解除する。これにより再生制限が解かれ、ストレージ 1 8 に記録されているデータはパケット分離部 1 6 でパケットが分離される。パケット分離されたデータは MPEG デコーダ 1 7 で圧縮が解凍された後、デジタル／アナログ変換されて音声信号及び映像信号 A/V として TV に出力される。

【0010】ところが現行の放送形態におけるセキュリティシステムで、上述のようにストレージ 1 8 にソフトウェア情報をダウンロードしておき、観たいときにこのソフトウェア情報を鑑賞し得るようなシステムを実現しようとする、以下のような問題点が生ずる。

【0011】すなわち現行のデジタル信号伝送システムでは、図 1 1 に示すように、暗号解除部 1 5 で暗号を解除した後にストレージ 1 8 にソフトウェア情報をダウンロードする場合（図 1 1 の A 点）、暗号を解除することはすなわち課金することであるので、有料ソフトを課金なしに暗号を解除してストレージ 1 8 にダウンロードすることはできない。ここで課金情報だけを無料として全てのデータの暗号を解除してストレージ 1 8 にダウンロードすると、1 つのソフトウェア情報についてはそのままスルーで端末 1 0 より出力されてしまう。

【0012】またストレージ 1 8 が端末 1 0 に内蔵されておらず端末 1 0 に接続され、暗号解除部 1 5 とパケット分離部 1 6 との間にスイッチング手段が設けられていない場合には、暗号を全て解除してストレージ 1 8 にダウンロードすると、暗号が解除されたデータが全て送出され、図 1 1 の C 点において契約者以外の者にただで観られるおそれがあった。

【0013】このような問題点を解決するために、暗号を解除する前、すなわちデマルチプレクサ 1 4 で多重化が解除された後（図 1 1 の B 点）、ストレージ 1 8 にダウンロードすることが考えられる。ところがデマルチプレクサ 1 4 で多重化が解除された後ストレージ 1 8 にダウンロードすると、暗号化されたままの状態であるので I (intra-coded) ピクチャを抜き出すことができず、変速再生することができないという問題があった。

【0014】また放送系でデータを暗号化するシステムでは、セキュリティを確保するために 1 年とか 2 年毎にキーを変えるため、ストレージ 1 8 にソフトウェア情報をダウンロードした後にキーの変更があった場合、暗号を解除することができずダウンロードしたソフトウェア情報を観ることができないという問題があった。

【0015】本発明は以上の点を考慮してなされたもの

で、有料のソフトウェア情報を伝送する場合のセキュリティを確保し得るデジタル信号伝送方法、デジタル信号受信装置及び記録媒体を提案しようとするものである。

【 0 0 1 6 】

【課題を解決するための手段】かかる課題を解決するため本発明においては、少なくとも映像信号を帯域圧縮符号化したデジタル信号に暗号化処理をして伝送するデジタル信号伝送方法において、所定のサービスを提供する映像を伝送する場合には、帯域圧縮符号化したデ

ジタル信号に第 1 の暗号化処理をした後、当該第 1 の暗号化処理がなされたデジタル信号にさらに暗号化処理をして伝送する。

【 0 0 1 7 】また本発明においては、少なくとも映像信号を帯域圧縮符号化したデジタル信号に暗号化処理をして伝送するデジタル信号伝送方法において、帯域圧縮符号化されかつ暗号化処理されたデジタル信号と、所定映像単位内で帯域圧縮符号化が完結しているデ

ジタル信号とを混合して伝送する。

【 0 0 1 8 】また本発明においては、少なくとも映像信号を帯域圧縮符号化したデジタル信号に第 1 の暗号をかけた後、第 2 の暗号をかけて放送局より伝送されるデジタル信号を受信するデジタル信号受信装置 (4 0) において、デジタル信号にかけられた第 2 の暗号を解除する第 2 の暗号解除手段 ((1 5) 、 (1 9)) と、当該第 2 の暗号が解除されたデジタル信号を記録媒体に記録すると共に、当該記録媒体に記録されたデジタル信号を再生する記録再生手段 ((7 3) 、 (7 4) 、 (7 5) 、 (7 6) 、 (7 7)) と、記録媒体より再生される再生信号の第 1 の暗号を解除する第 1 の暗号解除手段 ((4 6) 、 (9 1)) とを設ける。

【 0 0 1 9 】また本発明においては、少なくとも映像信号を帯域圧縮符号化したデジタル信号に暗号化処理をした信号が記録されている記録媒体 (1 0 1) を設ける。

【 0 0 2 0 】

【作用】所定のサービスを提供する映像を伝送する場合、映像信号を帯域圧縮符号化したデジタル信号に第 1 の暗号化処理をした後、当該デジタル信号にさらに暗号化処理をして伝送する。これにより、映像信号に 2 重のセキュリティを付加することかできるので、一段とセキュリティが確保されたデジタル信号伝送方法を実現し得る。

【 0 0 2 1 】また少なくとも映像信号を帯域圧縮符号化しかつ暗号化処理したデジタル信号と、所定映像単位内で帯域圧縮符号化が完結しているデジタル信号とを放送局 (3 0) で混合する。これにより、端末 (4 0) で変速再生処理をせずに変速再生画を観ることができ

る。

【 0 0 2 2 】少なくとも映像信号を帯域圧縮符号化した

デジタル信号に第 1 の暗号及び第 2 の暗号をかけて放送局 (3 0) より伝送されるデジタル信号を受信すると、受信したデジタル信号にかけられた第 2 の暗号を第 2 の暗号解除手段 ((1 5) 、 (1 9)) で解除した後、当該第 2 の暗号が解除されたデジタル信号を記録再生手段 ((7 3) 、 (7 4) 、 (7 5) 、 (7 7)) によつて記録媒体に記録する。再生時には、記録媒体より再生される再生信号の第 1 の暗号を第 1 の暗号解除手段 ((4 6) 、 (9 1)) で解除する。これにより、セキュリティが一段と確保されたデジタル信号受信装置 (4 0) を実現し得る。

【 0 0 2 3 】また少なくとも映像信号を帯域圧縮符号化したデジタル信号に暗号化処理をした信号が記録されている記録媒体 (1 0 1) を用意する。これにより、契約ユーザは暗号がかけられたソフトウェア情報が記録された記録媒体 (1 0 1) をローコストで入手することができ、観たい部分だけを課金処理して楽しむ新しいソフトウェア供給システムを構築することができる。

【 0 0 2 4 】

【実施例】以下図面について、本発明の一実施例を詳述する。

【 0 0 2 5 】 (1) デジタル信号伝送装置及びデジタル信号受信装置の構成

図 9 との対応部分に同一符号を付して示す図 1 において、3 0 は全体として本発明の実施例によるデジタル信号伝送装置を示している。デジタル信号伝送装置 3 0 すなわち放送局においては、所定のサービス例えば有料のソフトウェア情報を伝送する場合、予めソフトウェアデータにストレージ系の暗号をかけた後、当該ソフトウェアデータにさらに放送系の暗号をかけて 2 重のセキュリティを確保している。

【 0 0 2 6 】デジタル信号伝送装置 3 0 はデジタル信号送出部 3 1 及びソフトウェア供給部 3 2 によつて構成されている。デジタル信号伝送装置 3 0 において、ユーザより有料のソフトウェア情報、例えば映像ソフト、音楽ソフト、電子番組表、ショッピング情報、ゲームソフトや教育情報などが要求された場合には、図 1 に示すように、プログラムソース P S₂ としてのこれらのソフトウェア情報がソフトウェア供給部 3 2 に入力される。

【 0 0 2 7 】ソフトウェア供給部 3 2 では、まずデジタル信号でなるソフトウェアデータ P S₂ を M P E G エンコーダ 3 3 で帯域圧縮符号化する。帯域圧縮符号化されたデジタル信号はパケット生成部 3 4 及びトリックプレイ処理部 3 5 に入力される。トリックプレイ処理部 3 5 では映像データについて変速再生処理すなわち I (i n t r a - c o d e d) ピクチャを抜き出す処理をして、抜き出した I ピクチャをマルチプレクサ 3 6 に入力する。ここで M P E G 方式で帯域圧縮符号化された映像を変速再生し得るようにするための技術については、特願平 5 - 2 8 7 7 0 2 号

に記載されている。

【0028】パケット生成部34では、入力されたデジタル信号を映像データ、音声データ及びこれ以外のデータ毎にパケット化してマルチプレクサ36で多重化する。このマルチプレクサ36で映像データに1ピクチャが埋め込まれる。多重化されたデジタル信号は暗号化処理部37でストレージ系の暗号をかけた後送出部31のマルチプレクサ4に送出される。

【0029】マルチプレクサ4では、ストレージ系の暗号がかけられたデジタル信号を多重化し、暗号化処理部5でこの多重化されたデジタル信号に放送系の暗号をかける。従つてデジタル信号伝送装置30より送出されるデジタル信号には、ストレージ系の暗号と放送系の暗号が2重にかけられている。ここで送出部31で各プログラムに付加されるキーデータは全て共通であり、放送による課金データは無料である。

【0030】この2重のセキュリティが付加されたデジタル信号は、図10との対応部分に同一符号を付して示す図2に示すように、衛星8より直接又は衛星8より配信局9を介して家庭内に設置された端末、すなわちデジタル信号受信装置40に送られる。デジタル信号受信装置40では、スマートカード19をアクセスすることによつて、伝送されるデジタル信号にかけられた放送系の暗号を解除し、当該デジタル信号をデジタルストレージ41にダウンロードすることができる。すなわち伝送されるデジタル信号は、暗号解除部15において放送系の暗号が解除された後、デジタルストレージ41に記録される。

【0031】この場合、デジタルストレージ41にダウンロードされるデジタル信号には、ストレージ系の暗号だけが加かつた状態で記録され、しかも変速再生処理がなされた状態で記録される。従つて送出部31で付加された放送系のキーが変更されても影響はなく、また図2のC点においてはストレージ系の暗号がかかっているため映像をただで観られることはない。

【0032】ストレージ41にダウンロードされたソフトウェア情報PS₂を観る場合には、放送系とは別に登録されたID番号を入力する(例えばパーソナルコンピュータの画面上でID番号を入力する)ことにより、CPU42がモデム43を介してソフトウェア情報用の許可センタ44(図1)に登録の問い合わせをする。ここでCPU42は通常契約によるプログラムPS₁については放送系の許可センタ22に登録の問い合わせをし、ソフトウェア情報PS₂についてはソフトウェア系の許可センタ44に登録の問い合わせをする。すなわちCPU42はモデム43のシエアを制御することにより、放送系とソフトウェア系の2つの独立した課金体系を構築している。

【0033】許可センタ44はID番号をソフトウェア供給部32のコンディショナルアクセス45(図1)に

送つて登録を確認する。許可センタ44が登録を確認すると課金処理がなされ、CPU42はローカルコンディショナルアクセス46に暗号の解除を指示する。ここでローカルコンディショナルアクセス46はソフトウェア系の暗号を解除する機能を有する。これによりストレージ41の再生制限が解除されて暗号が解除され、ユーザは解除された部分だけ通常のVTR(video tape recorder)と同じ操作でソフトウェア情報を観ることができる。

【0034】(2)実施例によるデジタル信号伝送装置の構成

実施例によるデジタル信号伝送装置の送出部31及びソフトウェア供給部32の詳細構成をそれぞれ図3及び図4に示す。このデジタル信号伝送装置30において、通常契約のプログラムPS₁を供給する場合には、プログラムソースPS₁は送出部31に直接入力され、有料のソフトウェア情報を供給する場合には、当該ソフトウェア情報PS₂はソフトウェア供給部32を介して送出部31に供給される。

【0035】プログラムPS₁の鑑賞については、例えば業務用デジタルVTR47より供給されるプログラムの映像信号及び音声信号はそれぞれMPEGエンコーダ2A、2Bで帯域圧縮符号化された後、パケット生成部3A、3Bで画像及び音声毎にパケット化されてデータバス48を介してマルチプレクサ4に送出される。これと同時に、例えばパーソナルコンピュータ(以下パソコンと呼ぶ)49によつて映像データ及び音声データ以外のデータがデータインタフェース(データI/F)50を介してパケット生成部3Cに送出されてパケット化された後、データバス48を介してマルチプレクサ4に送出される。

【0036】またコンディショナルアクセス23よりキーデータがデータI/F51を介してパケット生成部3Dに送出されてパケット化され、データバス48を介してマルチプレクサ4に送出される。さらにコンディショナルアクセス23はソフトウェアデータを暗号化するためのキー情報を暗号化処理部5に送出する。マルチプレクサ4では、映像、音声及びこれ以外のデータを多重化し、暗号化処理部5において、コンディショナルアクセス23より入力されたキー情報に基づいてこの多重化されたデータに暗号をかける。暗号化されたデータはFEC部6でエラー訂正されて変調器7で変調された後、アンプコンバータ52を介して衛星8に伝送される。

【0037】これに対して有料のソフトウェア情報PS₂を伝送する場合には、図4に示すように、例えばデジタルVTR53より出力されるソフトウェア情報PS₂の映像信号及び音声信号はそれぞれMPEGエンコーダ33A、33Bで帯域圧縮符号化される。帯域圧縮符号化された映像信号はパケット生成部34A及びトリックプレイ処理部35に入力される。パケット生成部34

Aでは入力された映像信号をパケット化し、トリックプレイ処理部35では入力される映像信号より1ピクチャを抜き出して、この1ピクチャをマルチプレクサ36に出力する。

【0038】帯域圧縮符号化された音声信号はパケット生成部34Bでパケット化される。またパソコン54より入力される映像及び音声以外の一般データがデータ1/F55を介してパケット生成部34Cに送出される。またコンディショナルアクセス45はキーデータをデータ1/F56を介してパケット生成部34Dに送出すると共に、ストレージ系のキー情報を暗号化処理部37に送出する。

【0039】各パケット生成部34でそれぞれパケット化されたデータは、データバス57を介してマルチプレクサ36で多重化されると共に、映像データに1ピクチャが埋め込まれる。多重化されたデータは、暗号化処理部37において、コンディショナルアクセス45より入力されたキー情報に基づいて暗号化された後、送出部31のデータ1/F58(図3)を介してパケット生成部3Eに入力される。パケット生成部3Eでパケット化されたデータは、データバス48を介してマルチプレクサ4で多重化されて暗号化処理部5で放送系の暗号がかけられた後、FEC部6、変調器7及びアップコンバータ52で各処理がなされて衛星8より直接又は衛星8より配信局9を介して端末40に伝送される。

【0040】(3)実施例によるデジタル信号受信装置の構成

実施例によるデジタル信号受信装置40は、図2との対応部分に同一符号が付された図5及び図6に示すように、デジタル信号伝送装置30より送出されるデジタル信号を受信する受信部60(図5)と、受信部60で受信した信号を記録媒体に記録し再生する記録再生部61(図6)とによって構成されている。この実施例の場合、受信部60と記録再生部61とはデジタルインタフェース(デジタルI/F)62、63を介して接続されている。

【0041】受信部60では、衛星8より直接又は衛星8より配信局9を介して伝送されるデジタル信号は圧縮されたデジタル信号としてチューナ12Aに入力される。チューニングされたデジタル信号は、復調器12Bで復調されてFEC部12Cでエラー訂正された後、デマルチプレクサ14及び暗号解除部15でなる暗号解除ブロックに入力される。暗号解除ブロックでは、登録されたユーザだけがもつことのできるキーによって放送系の暗号が解除される。

【0042】放送系の暗号が解除された一般データ及び所定バイト長のパケットを単位として複数のプログラムチャンネルが時分割多重された画像データは、パケット分離部16又は記録再生部61に送出される。パケット分離部16に送出される経路と記録再生部61に送出さ

れる経路との切換えはスイッチング手段(図示せず)によって行われ、この実施例では、スイッチング手段が記録再生部61に切り換えられているものとする。ここで一般データには、例えばTVモニタ上でユーザインタフェースを司るためのテキストデータ、フオンデータ、イメージデータ、グラフィックデータや動画データなどが含まれる。

【0043】一般データはインタラクティブな処理を行うCPUブロック64にデータポートを介して入力される。CPUブロック64は、メインCPU42、EEPROM(electrically erasable programmable read only memory)65、モデムインタフェース(モデムI/F)66、モデム43、VRAM(video random access memory)67、GPU(graphic processor unit)68、ROM(read only memory)69及びDRAM(dynamic random access memory)70によって構成されている。ここでハードディスクを内蔵するシステムの場合には、一般データはCPUバスを介して一度ハードディスク内に格納される。これらの一般データはユーザが外部よりコントローラによって操作された指示に従ってCPU42で処理がなされ、必要な表示データが出力される。

【0044】一方画像データは、図6に示すようにデジタルI/F62、63を介して記録再生部61に入力された後、パケット分離部71でパケット分離される。パケット分離されたデータは、TBC(time base corrector)処理されて、フォーマット変換部72でフォーマットが変換される。フォーマット変換されたデータはエラー訂正されてローカルコンディショナルアクセス46を介して変調された後、記録/再生処理部73によってメカデツキ74内の記録媒体に記録される。ここで記録媒体としては、テープ及びディスクの双方が考えられ、例えばデジタルVCR、デジタルビデオディスク(DVD)、ハードディスクやミニディスクなどがある。

【0045】ユーザより再生の指示があつた場合には、CPU42からVCRコントローラ75にデジタルI/F62、63を介してコマンドが入力される。VCRコントローラ75はこのコマンドに基づいてドライバ76によってメカデツキ74を駆動させる。これにより記録媒体上の所望の絶対アドレスまでサーチが行われ、ATF(automatic tracking following)77によってトラッキングがとられて記録/再生処理部73によって記録媒体上に記録されたデータが再生される。ここで絶対アドレスは、伝送データに予め付加してもよく、またデジタル信号受信装置40内で付加してもよい。

【0046】記録/再生処理部73によって再生された再生信号は、復調された後ローカルコンディショナルアクセス46でストレージ系の暗号が解除される。ストレージ系の暗号が解除された再生信号はエラー訂正され

10

20

30

40

50

て、フォーマット変換部 7 2 でフォーマットが変換される。フォーマット変換された再生信号はパケット生成部 7 8 でパケット化され、デジタル 1 / F 6 3、6 2 を介してパケット分離部 1 6 に送出されてパケット分離される。パケット分離された再生信号は、音声信号及び映像信号毎にそれぞれ M P E G 音声デコーダ 1 7 A、M P E G 映像デコーダ 1 7 B で圧縮が解凍される。

【 0 0 4 7 】 圧縮が解凍された音声信号はデジタルアナログ変換器 (D A C) 7 9 でアナログ信号に変換されて出力される。圧縮が解凍された映像信号は N T S C (n a t i o n a l t e l e v i s i o n s y s t e m c o m m i t t e e) エンコーダ 8 0 でエンコードされる。また C P U ブロック 6 4 より N T S C エンコーダ 8 1 にユーザインタフェース等に関する一般データが入力され、当該エンコーダ 8 1 でエンコードされた一般データはエンコーダ 8 0 より出力される映像信号に付加されて出力される。

【 0 0 4 8 】 以上の構成において、ソフトウェア情報 P S₂ をデジタル信号受信装置 4 0 に伝送する場合に、ソフトウェア供給部 3 1 においてソフトウェア情報 P S₂ にソフトウェア系の暗号をかけた後、送出部 3 2 において放送系の暗号をかけて 2 重のセキュリティを確保した状態でデジタル信号受信装置 4 0 に伝送する。デジタル信号受信装置 4 0 では、ソフトウェア情報 P S₂ にかけている放送系の暗号を解除した後デジタルストレージ 4 1 に記録する。デジタルストレージ 4 1 に記録されたソフトウェア情報 P S₂ を観る場合には、許可センタ 4 4 で登録の確認をし、登録の確認がされると、ソフトウェア系の暗号が解除されてソフトウェア情報 P S₂ を観ることができる。

【 0 0 4 9 】 以上の構成によれば、放送系のキーデータを全て共通にすると共に放送による課金データを無料とし、ソフトウェア情報 P S₂ を端末 4 0 に供給する場合には、ソフトウェアデータ P S₂ に放送系及びソフトウェア系の暗号を 2 重にかけて伝送し、端末 4 0 ではソフトウェアデータ P S₂ の放送系の暗号を解除してデジタルストレージ 4 1 にダウンロードする。これにより、ソフトウェア情報 P S₂ をデジタルストレージ 4 1 にダウンロードする際には、ソフトウェア情報 P S₂ にソフトウェア系の暗号がかけられているのでセキュリティを確保することができる。

【 0 0 5 0 】 また上述の構成によれば、パケット分離部 1 6 に送出される経路と記録再生部 6 1 に送出される経路とを切り換えるスイッチング手段を設けたことにより、契約ユーザに対してはビデオオンデマンドと V T R の長所をあわせもつたデジタル信号伝送システムを提供することができる。

【 0 0 5 1 】 また上述の構成によれば、ソフトウェア供給部 3 2 でソフトウェア情報 P S₂ に変速再生処理を施してからデジタル信号受信装置 4 0 にソフトウェア情報 P S₂ を伝送したことにより、契約ユーザはストレー

ジ 4 1 に記録されたソフトウェア情報 P S₂ を変速再生することができる。

【 0 0 5 2 】 また上述の構成によれば、伝送路の空き時間帯又は空き伝送路を利用して複数本の有料ソフトウェア情報 P S₂ を端末 4 0 のストレージ 4 1 にダウンロードすることができるので、ユーザはダウンロードした複数本のソフトウェア情報 P S₂ のうち、観たい時間に観たいものだけを観ることができる。すなわち観たいソフトウェア情報 P S₂ を選択する毎に課金処理が行われてストレージ 4 1 内で再生制限が解除される。また衛星による伝送の場合のような 1 対 1 でないデジタル信号伝送システムにおけるビデオオンデマンドを実現する手段として有効である。

【 0 0 5 3 】 また上述の構成によれば、通常契約によるプログラム P S₁ についての課金情報を管理する許可センタ 2 2 へのアクセスとソフトウェア情報 P S₂ についての課金情報を管理する許可センタ 4 4 へのアクセスとの切換えをモデム 4 3 を介して制御したことにより、放送系とソフトウェア系の 2 つの独立した課金体系を構築することができる。

【 0 0 5 4 】 (4) 実施例によるデジタル信号伝送システム

図 1 及び図 2 との対応部分に同一符号を付して示す図 7 において、9 0 は全体として実施例によるデジタル信号伝送システムの概略構成を示している。デジタル信号伝送システム 9 0 では、所定のサービス例えば有料のソフトウェア情報 P S₂ を伝送する場合、ソフトウェア情報 P S₂ にストレージ系の暗号をかけた後、当該ソフトウェア情報 P S₂ にさらに放送系の暗号をかけて 2 重のセキュリティを確保すると共に、ストレージ系の暗号をかける際に用いる暗号化キー K_m をソフトウェア情報用のパーソナルキー K_p 2 を用いて暗号化している。

【 0 0 5 5 】 ユーザがデジタル信号伝送装置 3 0 より伝送されるプログラムソース P S₁ を観る場合、ユーザは放送局 3 0 より郵送で送られてくるスマートカード 1 9 を端末 4 0 に差し込み、登録された放送系の I D 番号 I D 1 を入力する。これにより、C P U 4 2 がモデム 4 3 を介して許可センタ 2 2 に登録の問い合わせをし、当該ユーザの登録が確認されると、放送局すなわちデジタル信号伝送装置 3 0 より放送系の暗号がかけられたプログラムソース E s (D a t a) が送られてくる。

【 0 0 5 6 】 すなわち放送局 3 0 では、プログラムソース P S₁ をデジタル信号受信装置 4 0 に伝送する場合、暗号化処理部 5 において暗号化キー K_s によつてプログラムソース P S₁ に放送系の暗号をかける。この暗号化キー K_s はワークキー (W o r k K e y、K_w) によつて暗号化され、またワークキー K_w はユーザ毎に与えられる放送系のパーソナルキー K_p 1 によつて暗号化される。従つて暗号化処理部 5 は、放送系の暗号がかけられたプログラムソース E s (D a t a) と、暗号化キー E (K

s) 及びワークキー E (Kw) とを多重化してデジタル信号受信装置 40 に伝送する。

【0057】スマートカード 19 には、暗号化キー Km を暗号化する際に用いられたパーソナルキー Kp1 が含まれている。従つて端末 40 では、暗号化されたワークキー E (Kw) の暗号がパーソナルキー Kp1 によつて解除され、この暗号が解除されたワークキー Kw によつて暗号化キー E (Ks) の暗号が解除される。さらにこの暗号が解除された暗号化キー Ks によつて、プログラムソース Es (Data) にかけている放送系の暗号が解除される。暗号が解除されたプログラムソース PS_i は MPEG デコーダ 17 で圧縮が解凍されてアナログ信号に変換された後、TV に出力される。

【0058】ユーザがソフトウェア情報 PS_i をデジタルストレージ 41 にダウンロードしたい場合 (この場合、上述のスイッチング手段はデジタルストレージ 41 に送出される経路に切り換わる)、ユーザはスマートカード 19 を端末 40 に差し込み、放送局 30 に登録された放送系の ID 番号 ID1 を入力する。これにより、CPU 42 がモデム 43 を介して許可センタ 22 に登録の問い合わせをし、当該ユーザの登録が確認されると、放送局 30 より放送系及びソフトウェア系の暗号がかけられたプログラムソース Es {Em (Data)} が送られてくる。

【0059】すなわち放送局 30 では、暗号化処理部 37 においてソフトウェア情報用の暗号化キー Km によつてソフトウェア情報 PS_i にストレージ系の暗号をかける。またこの暗号化キー Km はユーザ毎に与えられるソフトウェア情報用のパーソナルキー Kp2 によつて暗号化される。暗号化されたソフトウェアデータ Em (Data) は暗号化処理部 5 に送出され、暗号化された暗号化キー E (Km) は許可センタ 44 に送られる。

【0060】暗号化処理部 5 では、ソフトウェア系の暗号がかけられたソフトウェアデータ Em (Data) に暗号化キー Ks を用いて放送系の暗号をかける。上述のように、この暗号化キー Ks はワークキー Kw によつて暗号化され、ワークキー Kw はパーソナルキー Kp1 によつて暗号化される。暗号化処理部 5 は、ソフトウェア系及び放送系の暗号が 2 重にかけられたソフトウェアデータ Es {Em (Data)} と、暗号化キー E (Ks) 及びワークキー E (Kw) とを多重化して端末 40 に伝送する。

【0061】端末 40 では、当該端末 40 にスマートカード 19 が差し込まれているので、上述のように 2 重に暗号化されたソフトウェアデータ Es {Em (Data)} の放送系の暗号が解除される。放送系の暗号が解除されたソフトウェアデータ Em (Data) はデジタルストレージ 41 に記録される。

【0062】デジタルストレージ 41 に記録されたソフトウェアデータ Em (Data) を観る場合、ユーザはス

martカード 91 を端末 40 に差し込み、登録されたソフトウェア系の ID 番号 ID2 を入力する。これにより、CPU 42 がモデム 43 を介して許可センタ 44 に登録の問い合わせをする。当該ユーザの登録が確認されると、課金処理がなされた後、例えば電話回線を通じて許可センタ 44 より暗号化キー E (Km) がモデム 43 を通じてスマートカード 91 に入力され、暗号化キー E (Km) の暗号が解除される。

【0063】すなわちスマートカード 91 には、ソフトウェア系の暗号化キー Km を暗号化する際に用いたパーソナルキー Kp2 が含まれている。従つて暗号化キー E (Km) の暗号がパーソナルキー Kp2 によつて解除される。暗号が解除された暗号化キー Km は CPU 42 を介して暗号解除部 46 に送出される。

【0064】暗号解除部 46 では、暗号化キー Km によつてソフトウェアデータ Em (Data) にかけているソフトウェア系の暗号を解除して MPEG デコーダ 17 に送出する。MPEG デコーダ 17 では、暗号が解除されたソフトウェアデータ PS_i の圧縮を解凍してアナログ信号に変換した後、TV に出力する。

【0065】以上の構成において、ソフトウェア情報 PS_i をデジタル信号受信装置 40 に伝送する場合、ソフトウェア情報 PS_i にソフトウェア系の暗号をかけた後放送系の暗号をかけて伝送すると共に、ソフトウェア系の暗号をかける際に用いた暗号化キー Km をパーソナルキー Kp2 を用いて暗号化する。

【0066】デジタル信号受信装置 40 では、スマートカード 19 を用いてソフトウェアデータ Es {Em (Data)} の放送系の暗号を解除した後デジタルストレージ 41 に記録する。デジタルストレージ 41 に記録されたソフトウェアデータ Em (Data) を観る場合、スマートカード 91 によつて、暗号化キー E (Km) の暗号が解除され、暗号が解除された暗号化キー Km によつてソフトウェアデータ Em (Data) にかけているソフトウェア系の暗号が解除される。

【0067】以上の構成によれば、ソフトウェア情報 PS_i をデジタル信号受信装置 40 に伝送する際、ソフトウェア情報 PS_i にソフトウェア系の暗号及び放送系の暗号をかけると共に、ソフトウェア系の暗号をかける際に用いた暗号化キー Km をパーソナルキー Kp2 を用いて暗号化する。これにより、ソフトウェア情報 PS_i のセキュリティをさらに一段と確保することができる。

【0068】また上述の構成によれば、暗号化された暗号化キー E (Km) の暗号を解除するためのパーソナルキー Kp2 をスマートカード 91 に内蔵したことにより、ユーザは暗号化キー E (Km) の暗号を簡易かつ確実に解除することができるので、観たい時間に観たいソフトウェア情報 PS_i を観ることができる。

【0069】(5) 他の実施例

なお上述の実施例においては、契約ユーザが有料のソフ

トウェア情報を観る場合、契約ユーザは、ソフトウェア情報 P S₂ をストレージ 4 1 にダウンロードしておき、ユーザが観たいときにデジタルストレージ 4 1 に記録されたソフトウェア情報 P S₂ を観る場合について述べたが、本発明はこれに限らず、図 8 に示すようにソフトウェア供給部 3 2 及びデジタル信号受信装置 4 0 でパッケージ系システム 1 0 0 を構築し、ソフトウェア供給部 3 2 で暗号化したソフトウェア情報を記録媒体に記録してパッケージにし、このパッケージソフトウェア 1 0 1 を、例えば月極めなどで定期的にユーザに送つてもよい。

【0070】この場合、図 8 に示すように、デジタル信号受信装置 4 0 だけで課金のシステムを構築することができる。またユーザは暗号化された複数のソフトウェア情報が記録されたソフトウェアパッケージ 1 0 1 をローコストで入手することによつて、観たい部分だけを課金処理して楽しむというような、ソフトウェア情報のパッケージ化による新しいソフトウェア情報の供給システムを構築することができる。ここでパッケージソフトウェア 1 0 1 には例えば 10 本分の映画が記録されている。

【0071】また上述の実施例においては、放送系の許可センタ 2 2 及びソフトウェア系の許可センタ 4 4 を設けて、CPU 4 2 によつてモデム 4 3 のシェアを制御することにより、2 つのそれぞれ独立した課金体系を構築した場合について述べたが、本発明はこれに限らず、1 つの許可センタで放送系及びソフトウェア系のプログラムに対する課金処理を行つてもよい。

【0072】また上述の実施例においては、受信部 6 0 に記録再生部 6 1 が接続されたデジタル信号受信装置 4 0 を用いた場合について述べたが、本発明はこれに限らず、記録再生部 6 1 を内蔵したデジタル信号受信装置 4 0 を用いてもよい。

【0073】また上述の実施例においては、変速再生処理をソフトウェア供給部 3 2 で行つた場合について述べたが、本発明はこれに限らず、端末すなわちデジタル信号受信装置 4 0 で変速再生処理を行つてもよい。

【0074】また上述の実施例においては、通常契約によるプログラムソース P S₁ を観るためのスマートカード 1 9 と、ソフトウェア情報 P S₂ を観るためのスマートカード 9 1 を別個に設けた場合について述べたが、本発明はこれに限らず、1 枚のスマートカードにスマートカード 1 9 及びスマートカード 9 1 の機能をもたせてもよい。

【0075】また上述の実施例においては、ソフトウェア情報 P S₂ をデジタルストレージ 4 1 にダウンロードした場合について述べたが、本発明はこれに限らず、ソフトウェア情報 P S₂ をリアルタイムに観ることもできる。この場合、スイッチング手段をパケット分離部 1 6 に送出する経路に切り換えると共にスマートカード 1 9 及び 9 1 を端末 4 0 に差し込む。これにより、ソフト

ウェア情報 P S₂ にかけてられている放送系及びソフトウェア系の暗号が解除されてリアルタイムにソフトウェア情報 P S₂ を観ることができる。

【0076】また上述の実施例においては、音声信号及び映像信号を帯域圧縮符号化してデジタル信号受信装置 4 0 に伝送した場合について述べたが、本発明はこれに限らず、映像信号だけを帯域圧縮符号化してデジタル信号受信装置 4 0 に伝送してもよい。

【0077】

【発明の効果】上述のように本発明によれば、所定のサービスを提供する映像を伝送する場合、映像信号を帯域圧縮符号化したデジタル信号に第 1 の暗号化処理をした後、当該デジタル信号にさらに暗号化処理をして伝送することにより、映像信号に 2 重のセキュリティを付加することができるので、一段とセキュリティが確保されたデジタル信号伝送方法を実現し得る。

【図面の簡単な説明】

【図 1】本発明の実施例によるデジタル信号伝送装置の構成を示すブロック図である。

【図 2】本発明の実施例によるデジタル信号受信装置の構成を示すブロック図である。

【図 3】実施例によるデジタル信号伝送装置の送出部の詳細構成を示すブロック図である。

【図 4】実施例によるデジタル信号伝送装置のソフトウェア供給部の詳細構成を示すブロック図である。

【図 5】実施例によるデジタル信号受信装置の受信部の詳細構成を示すブロック図である。

【図 6】実施例によるデジタル信号受信装置の記録再生部の詳細構成を示すブロック図である。

【図 7】実施例によるデジタル信号伝送システムの概略構成を示すブロック図である。

【図 8】パッケージ系のソフトウェア供給システムの説明に供するブロック図である。

【図 9】従来のデジタル信号伝送装置の構成を示すブロック図である。

【図 10】従来のデジタル信号受信装置の構成を示すブロック図である。

【図 11】従来のデジタル信号受信装置においてソフトウェア情報をダウンロードする際の問題点の説明に供するブロック図である。

【符号の説明】

1、30……デジタル信号伝送装置、2、2A、2B、33、33A、33B……MPEG エンコーダ、3、3A、3B、3C、3D、3E、34、34A、34B、34C、34D、78……パケット生成部、4、36……マルチプレクサ、5、37……暗号化処理部、6、12C……FEC 部、7……変調器、8……衛星、9……配信局、10、40……デジタル信号受信装置、11……アンテナ、12……フロントエンド部、12A……チューナ、12B……復調器、13……データ

17

取出し部、14……デマルチプレクサ、15……暗号解除部、16、71……パケット分離部、17……MPEGデコーダ、17A……MPEG音声デコーダ、17B……MPEG映像デコーダ、18、41……デジタルストレージ、19、91……スマートカード、20、42……CPU、21、43……モデム、22、44……許可センタ、23、45……コンディショナルアクセス、24、46……ローカルコンディショナルアクセス、31……送出部、32……ソフトウェア供給部、35……トリックプレイ処理部、47、53……デジタルVTR、48、57……データバス、49、54……パーソナルコンピュータ、50、51、55、56、5

18

8……データインタフェース、52……アップコンバータ、60……受信部、61……記録再生部、62、63……デジタルインタフェース、64……CPUブロック、65……EEPROM、66……モデムインタフェース、67……VRAM、68……GPU、69……ROM、70……DRAM、72……フォーマット変換部、73……記録/再生処理部、74……メカデツキ、75……VCRコントローラ、76……ドライバ、77……ATF、79……DAC、80、81……NTSCエンコーダ、90……デジタル信号伝送システム、100……パッケージ系システム、101……パッケージソフトウェア。

【図1】

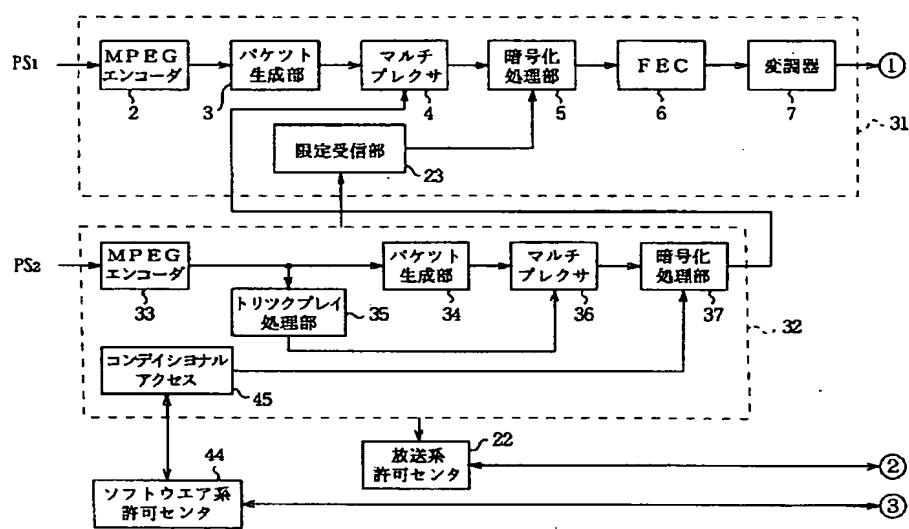


図1 デジタル信号伝送装置の構成

【図9】

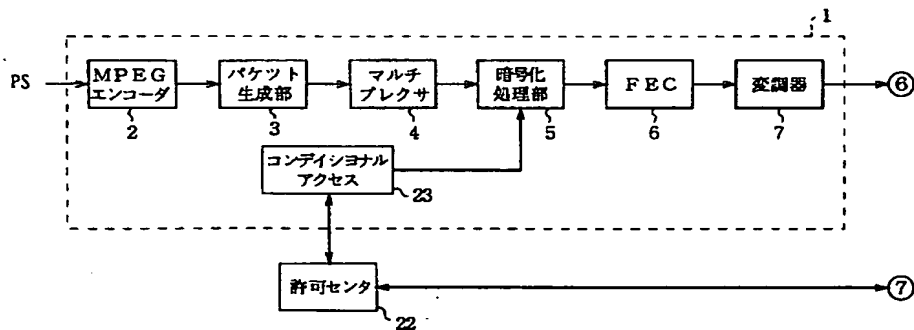


図9 従来のデジタル信号伝送装置

【図 2】

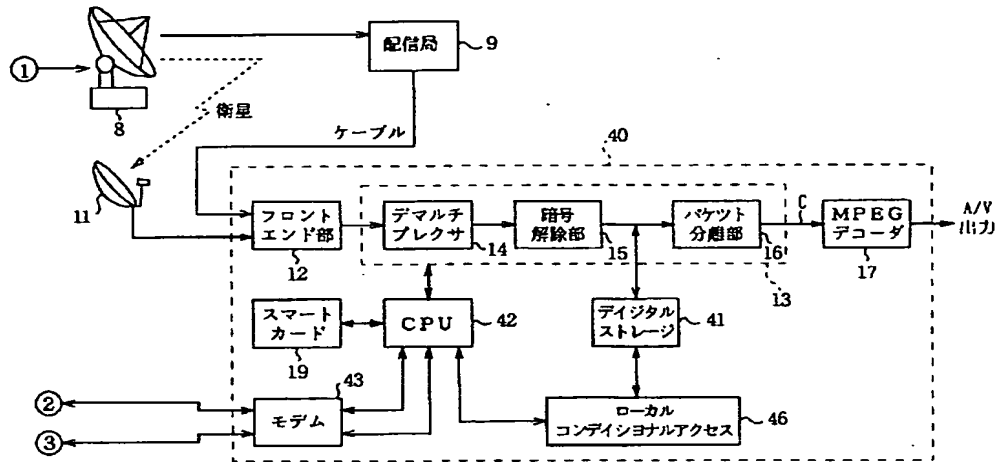


図 2 デジタル信号受信装置の構成

【図 3】

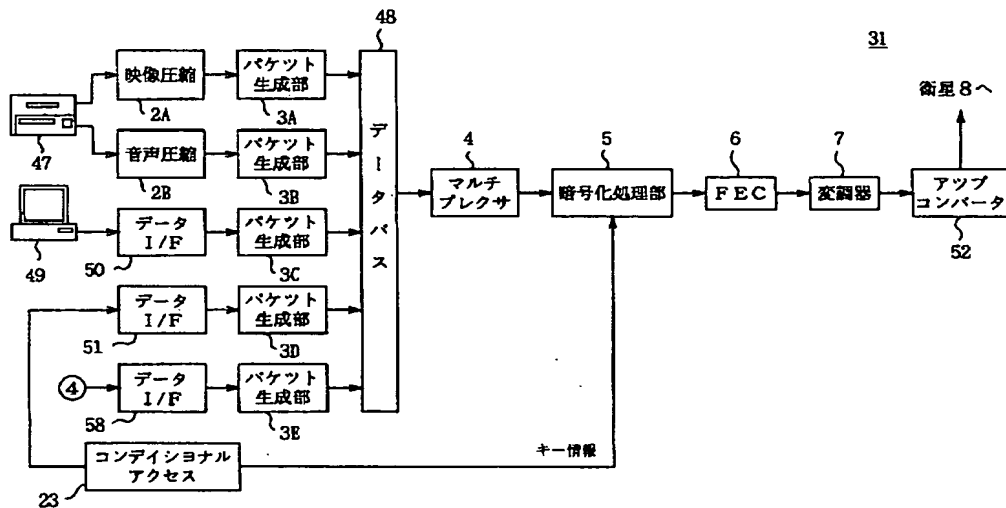


図 3 実施例によるデジタル信号伝送装置の送出部の構成

【図 4】

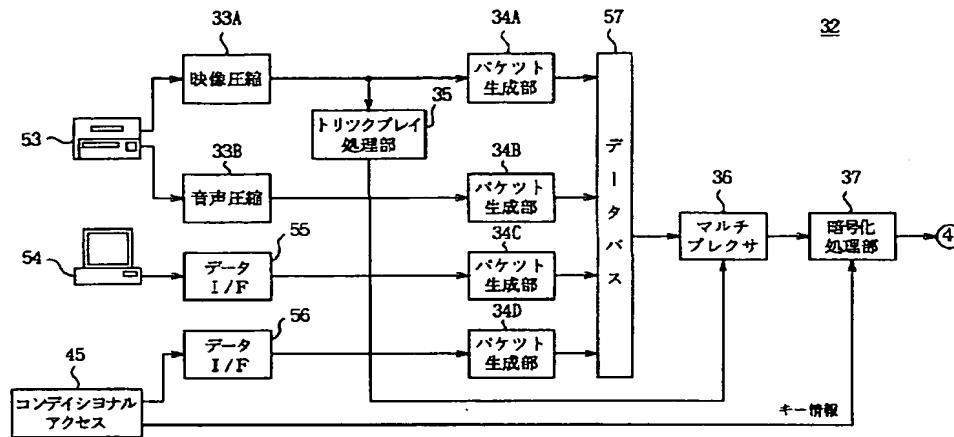


図 4 実施例によるデジタル信号伝送装置のソフトウェア供給部の構成

【図 5】

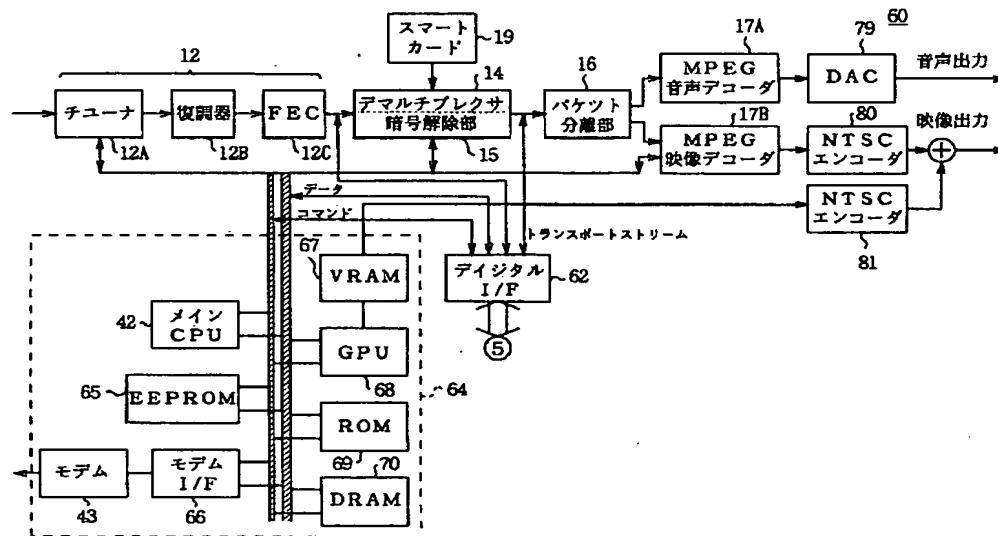


図 5 実施例によるデジタル信号受信装置の受信部の構成

【圖 7】

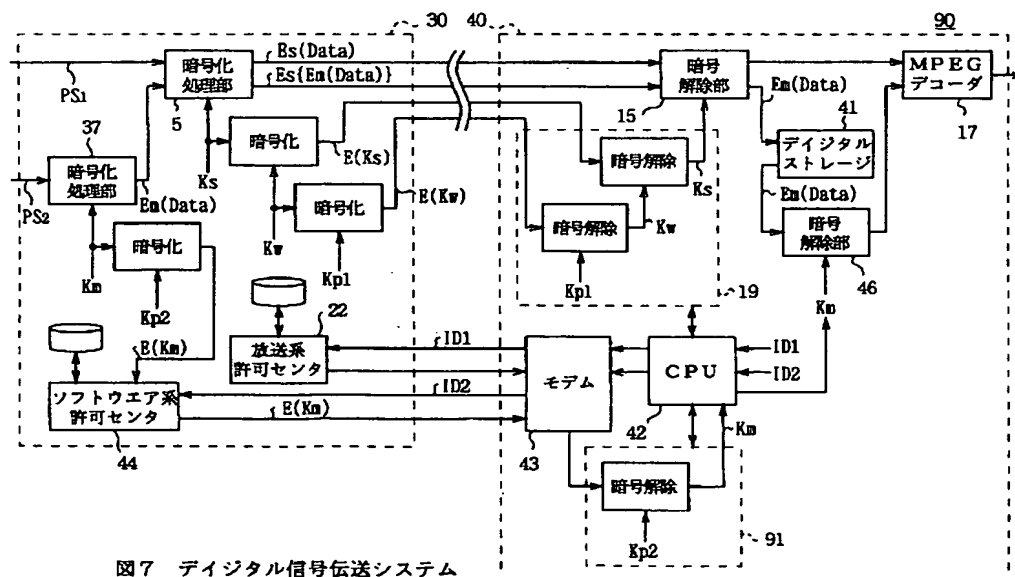


図7 デジタル信号伝送システム

【図 8】

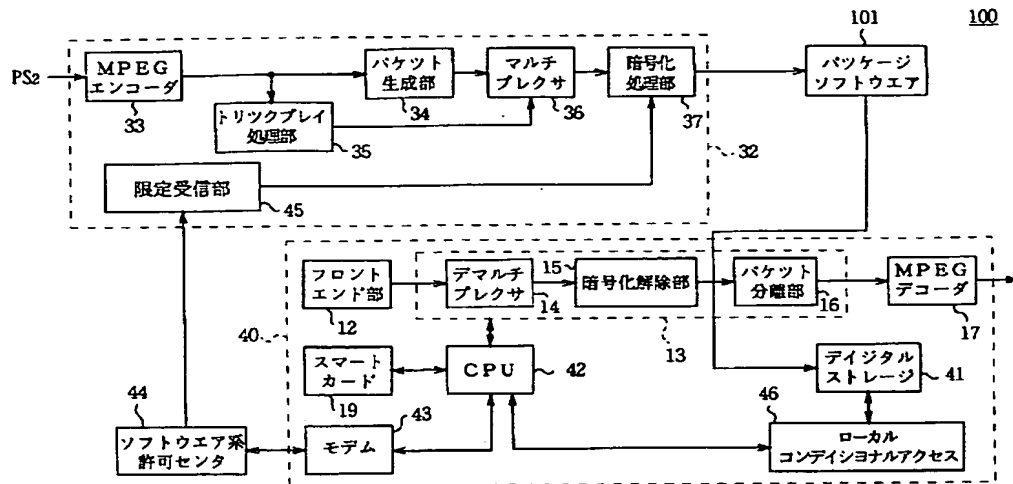


図 8 パッケージ系のソフトウェア供給システム

【図 10】

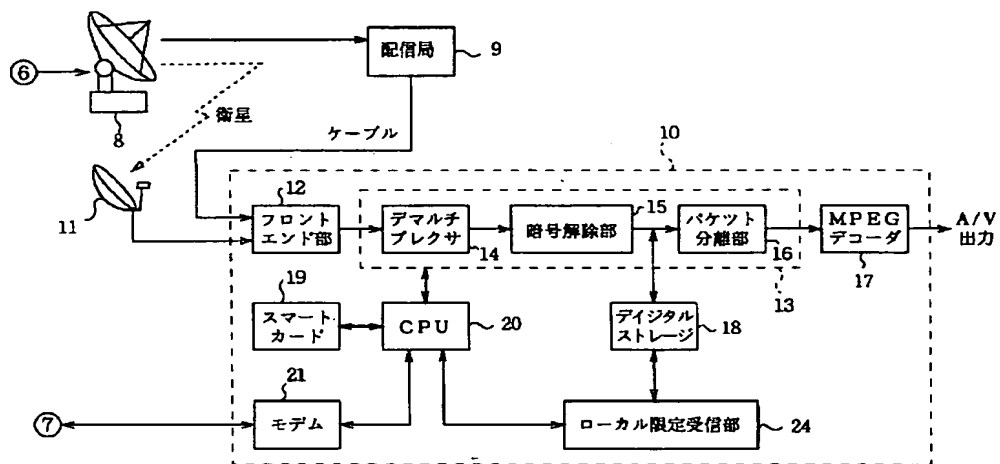


図 10 従来のデジタル信号受信装置

【図 1 1】

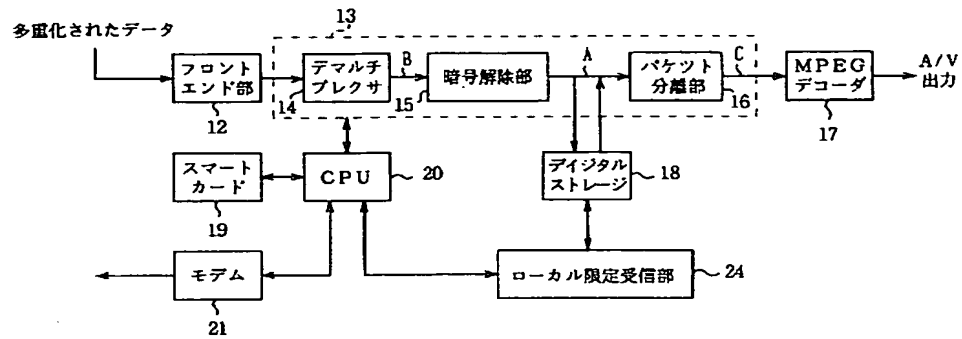


図 1 1 従来のデジタル信号受信装置

フロントページの続き

(51) Int. Cl. ⁶

H 0 4 H 1/00

H 0 4 N 7/167

識別記号

庁内整理番号

F I

技術表示箇所

F